UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

Tiffany Rayburn and Marquita Patterson on behalf of themselves individually and on behalf of all others similarly situated, Plaintiffs, v. MERS Missouri Goodwill Industries, Defendant.	**CASE NO.** 4:24-cv-756 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Tiffany Rayburn and Marquita Patterson ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant MERS Missouri Goodwill Industries ("MERS" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of current and former employees' personally identifiable information and personal health information, including full names, dates of birth, Social Security numbers, and medical diagnosis information (collectively the "PII/PHI").[1]

[1] MERS Goodwill Notice of Data Security Incident, MERS Missouri Goodwill Industries, https://mersgoodwill.org/notice-of-data-security-incident/ (last visited May 28, 2024).

3. On information and belief, the Data Breach occurred between March 10, 2023 and March 15, 2023. However, it is unclear when MERS became aware of the breach due to the obfuscating nature of its breach notice.

4. On May 9, 2024, over a year and two months after the breach occurred, MERS finally notified Plaintiffs and Class Members about the widespread Data Breach ("Notice Letter"). Plaintiff Patterson's Notice Letter is attached as **Exhibit A**. A standard Notice Letter is attached as **Exhibit B.**

5. MERS waited over fourteen months after the Data Breach began before informing Class Members, even though Plaintiffs and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. MERS' Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell victims how many people were impacted, how the breach happened on MERS' systems, when MERS discovered the Data Breach, or why it took MERS fourteen months to begin notifying victims that hackers had gained access to highly sensitive PII/PHI.

7. Defendant's failure to timely detect and report the Data Breach made its current and former employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII/PHI.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII/PHI misuse.

9. In failing to adequately protect Plaintiffs' and the Class's PII/PHI, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees.

10. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII/PHI. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiffs are Data Breach victims.

12. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Marquita Patterson, is a natural person and citizen of Missouri, where she intends to remain.

14. Plaintiff, Tiffany Rayburn, is a natural person and citizen of Missouri, where she intends to remain.

15. Defendant, MERS, is a Missouri non-profit organization with its principal place of business at 1727 Locust Street, St. Louis, MO 63103.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

MERS

19. MERS is a non-profit organization that offers programs and services including career counseling, skills training, education and literacy programs, employment services, and more.[2] MERS boasts a total annual revenue of $224 million.[3]

20. As an organization that annually serves more than 11,000 individuals and operates over 42 career centers,[4] MERS understood the need to protect its own employees' data, as well as prioritize its data security.

21. Indeed, MERS promises in its privacy policy that it "recognizes the importance of protecting information we may collect." Defendant also states that in order to "prevent unauthorized access, maintain data accuracy, and to ensure the appropriate use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect."[5]

---

[2] About, MERS Goodwill, https://mersgoodwill.org/about/ (last visited May 28, 2024).
[3] MERS Goodwill, ProPublica, https://projects.propublica.org/nonprofits/organizations/430652657 (last visited May 28, 2024).
[4] Home, MERS Goodwill, https://mersgoodwill.org/ (last visited May 28, 2024).
[5] Privacy Policy, MERS Goodwill, https://mersgoodwill.org/privacy-policy/ (last visited May 28, 2024).

22. Despite recognizing its duty to do so, on information and belief, MERS has not implemented reasonably cybersecurity safeguards or policies to protect its current and former employees' PII/PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, MERS leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to current and former employees' PII/PHI.

The Data Breach

23. As a condition of employment with MERS, Defendant requires its employees, including Plaintiffs, to disclose PII including but not limited to, their names, dates of birth, and Social Security numbers. Defendant used that PII to facilitate its employment of Plaintiffs, including payroll, and required Plaintiffs to provide that PII to apply for employment and payment for that employment.

24. On information and belief, Defendant collects and maintains current and former employees' PII/PHI in its computer systems.

25. In collecting and maintaining PII/PHI, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

26. According to the Breach Notice, on or about March 10, 2023, "an unauthorized party accessed and removed a limited number of files from [MERS'] computer systems." An internal investigation revealed that the files were not only accessed but also "removed by the unauthorized party." Ex. A

27. In other words, MERS' investigation revealed that its network had been hacked by cybercriminals an appalling fourteen months before notice was sent to victims and that Defendant's

cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of current and former employees' highly private PII/PHI.

28. Most data breach notice letters will, at minimum, admit to the date of the breach as well as when the breach was discovered. Not Defendant. Instead, Defendant intentionally obfuscates the appallingly long period between the date of the Breach and when Defendant discovered it, leaving Plaintiffs and Class Members in the dark.

29. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's PII/PHI for theft and sale on the dark web.

30. On or around May 9, 2024—an astonishing one year and two months after the Breach first occurred – MERS finally notified Plaintiffs and Class Members about the Data Breach.

31. Despite its duties and alleged commitments to safeguard PII/PHI, Defendant did not in fact follow industry standard practices in securing current and former employees' PII/PHI, as evidenced by the Data Breach.

32. In response to the Data Breach, Defendant contends that it "continue[s] to take significant measures to protect your information." Ex. A. Although Defendant fails to expand on what these alleged "measures" are, such steps should have been in place before the Data Breach.

33. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it recommended "placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report" and encouraged breach victims to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis." Ex. B.

34. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect current and former employees PII/PHI, insisting

that, despite the Data Breach demonstrating otherwise, Defendant is "committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it." Ex. B.

35. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII/PHI. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

36. On information and belief, MERS has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII/PHI that cannot be changed, such as Social Security numbers.

37. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII/PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

38. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they suffered and will suffer.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII/PHI. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI.

Royal claims credit—and publishes the stolen PII/PHI

40. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII/PHI appear to be the notorious cybercriminal group "Royal" ransomware group.[6]

41. On March 27, 2023, Royal ransomware group claimed credit for the Data Breach on its Dark Web website.[7]

42. Thereafter, Royal ransomware indicated it would *publish* the stolen PII/PHI, stating "we are ready to share some info with you" and providing a link to the files.

43. Thus, it appears Plaintiffs' and Class members' PII/PHI was already published on the Dark Web.

44. Royal ransomware group emerged in early 2022 and is suspected to consist of former members of other ransomware groups. It is reported to be the "most prolific ransomware in the e-crime landscape, overtaking Lockbit for the first time in more than a year."[8]

---

[6] This Week in Ransomware: May 17, 2024, Comparitech, https://www.comparitech.com/news/the-week-in-ransomware-may-17-2024/ (last visited May 29, 2024).
[7] FalconFeeds, Twitter, https://x.com/FalconFeedsio/status/1641032465388011523 (last visited May 29, 2024).
[8] Royal Rumble: Analysis of Royal Ransomware, Cybereason, https://www.cybereason.com/blog/royal-ransomware-analysis (last visited May 29, 2024).

45. Thus, the Cybersecurity and Infrastructure Security Agency (CISA) and FBI have warned that Royal:

a. "uses its own custom-made file encryption program";

b. does "not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor"; and

c. "has targeted over 350 known victims worldwide and ransomware demands have exceeded 275 million USD."[9]

46. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

47. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the industry preceding the date of the breach.

48. In light of recent high profile data breaches at other companies in its industry, Defendant knew or should have known that its electronic records and current and former employees' PII/PHI would be targeted by cybercriminals.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[10] The 330 reported

[9] #StopRansomware: Royal Ransomware, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[10] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).

breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[11]

50. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [12]

51. Cyberattacks on companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including MERS.

Plaintiff Patterson's Experience

53. Plaintiff Patterson is a former employee of MERS.

54. Plaintiff Patterson received MERS' Breach Notice in or around May 2024.

55. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for fourteen months.

---

[11] *Id*.

[12] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).

[13] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

56. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff' for theft by cybercriminals and sale on the dark web.

57. Upon information and belief, through its Data Breach, Defendant compromised at least Plaintiff's full name, date of birth, and Social Security number.

58. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

59. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed in the Data Breach.

60. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

61. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

62. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

63. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties and possibly criminals.

64. Indeed, following the Data Breach, Plaintiff's bank card was fraudulently used to make unauthorized purchases. These fraudulent transactions suggest that her PII, including her bank account information, which was provided to Defendant during her employment, has been stolen as a result of the Data Breach and is now in the hands of cybercriminals.

65. Further, following the Data Breach, Plaintiff has experienced a dramatic increase in spam calls and emails, suggesting that her PII/PHI is now in the hands of cybercriminals.

66. Once an individual's PII/PHI is for sale and access on the dark web, as Plaintiff's PII/PHI is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[14] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

67. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Rayburn's Experience

68. Plaintiff Rayburn is a former employee of MERS'.

69. Plaintiff received MERS' Breach Notice on or around May 2024.

70. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for fourteen months.

71. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII/PHI for theft by cybercriminals and sale on the dark web.

[14] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

72. Upon information and belief, through its Data Breach, Defendant compromised at least Plaintiff's full name, date of birth, and Social Security number.

73. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, contacting credit bureaus, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

74. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed in the Data Breach.

75. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

76. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

77. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

78. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties and possibly criminals.

79. Indeed, following the Data Breach, Plaintiff spent time contacting credit bureaus to determine whether her credit was impacted by the Data Breach. She was informed by the credit bureau that there were multiple unauthorized hard inquiries on her credit report since 2023 that she did not recognize. The credit bureau also informed Plaintiff that a P.O. box address was being used in connection with her name and an unauthorized actor was using the name "Tiffany Smith" to commit acts of fraud using Plaintiff's information.

80. Following the Data Breach, Plaintiff has experienced numerous instances of fraud in the form of an unauthorized actor fraudulently taking out loans, mortgages, and credit cards with Plaintiff's information, including:

a. In April 2023, an unauthorized actor fraudulently took out a mortgage in Plaintiff's name;

b. In April 2023, 10 credit cards were fraudulently taken out in Plaintiff's name, including a credit card with Chase bank;

c. In May 2023 an unauthorized actor fraudulently took out a loan in Plaintiff's name in Las Vegas; and

d. In February 2024, a car loan was fraudulently taken out in Plaintiff's name.

81. Following the Data Breach, Plaintiff has also experienced an enormous increase in spam calls, emails, and mail, including calls trying to convince Plaintiff to make purchases, calls claiming to be insurance companies, and mail that claims that Plaintiff purchased a car. This suggests that her PII/PHI has been stolen and is now in the hands of cybercriminals.

82. Once an individual's PII/PHI is for sale and access on the dark web, as Plaintiffs' PII/PHI is here as a result of the Breach, cybercriminals are able to use the stolen

and compromised to gather and steal even more information.[15] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

83. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

84. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII/PHI that can be directly traced to Defendant.

85. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII/PHI is used;

b. The diminution in value of their PII/PHI;

c. The compromise and continuing publication of their PII/PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

[15] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII/PHI; and

h. The continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII/PHI in its possession.

86. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

87. The value of Plaintiffs' and the Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years, and criminals frequently post stolen PII/PHI openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

88. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

89. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.

90. Cyber-criminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

91. The development of "Fullz" packages means that stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

92. Defendant disclosed the PII/PHI of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

93. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

94. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII/PHI.

95. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII/PHI that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

96. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

97. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

98. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its current and former employees' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

100. As noted above, experts studying cyber security routinely identify entities in possession of PII/PHI as being particularly vulnerable to cyberattacks because of the value of the PII/PHI which they collect and maintain.

101. Several best practices have been identified that a minimum should be implemented by employers in possession of PII/PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

102. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

103. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

104. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Violated HIPAA

105. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[16]

106. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[17]

107. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

[16] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[17] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures

with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

108. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

109. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the MERS Data Breach including all those who received notice of the breach.

110. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

111. Plaintiffs reserve the right to amend the class definition.

112. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of

hundreds of current and former employees whose PII/PHI was compromised in the Data Breach.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

    i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

    ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

    iii. Whether Defendant were negligent in maintaining, protecting, and securing PII/PHI;

    iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII/PHI;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

113. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

114. Plaintiffs reallege all previous paragraphs as if fully set forth below.

115. Plaintiffs and members of the Class entrusted their PII/PHI to Defendant. Defendant owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the PII/PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

116. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII/PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII/PHI —just like the Data Breach that ultimately came to pass. Defendant

acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII/PHI by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

117. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII/PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

118. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

119. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

120. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom

Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and the Class's PII/PHI.

121. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

122. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

123. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII/PHI of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

124. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their

PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

125. Plaintiffs reallege all previous paragraphs as if fully set forth below.

126. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII/PHI.

127. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII/PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's PII/PHI.

128. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

129. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII/PHI.

130. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

131. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

132. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

133. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

134. Had Plaintiffs and the Class known that Defendant did not adequately protect their PII/PHI, Plaintiffs and members of the Class would not have entrusted Defendant with their PII/PHI.

135. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

136. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII/PHI; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII/PHI, entitling them to damages in an amount to be proven at trial.

137. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII/PHI in its continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs reallege all previous paragraphs as if fully set forth below.

139. Plaintiffs and Class Members were required to provide their PII/PHI Defendant as a condition of applying and receiving employment from Defendant. Plaintiffs and Class Members provided their PII/PHI to Defendant in exchange for Defendant's employment and application for employment.

140. Plaintiffs and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII/PHI.

141. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII/PHI to Defendant in exchange for an application for employment and employment.

142. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

143. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

144. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

145. After all, Plaintiffs and Class Members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

146. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

147. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

148. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

149. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, receive and maintained.

150. In these and other ways, Defendant violated its duty of good faith and fair dealing.

151. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

152. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

153. Plaintiffs reallege all previous paragraphs as if fully set forth below.

154. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing PII/PHI to Defendant.

155. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII/PHI, as this was used to facilitate its services to Plaintiffs and the Class.

156. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII/PHI.

157. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

158. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class's PII/PHI because Defendant failed to adequately protect their PII/PHI.

159. Plaintiffs and Class Members have no adequate remedy at law.

160. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs reallege all previous paragraphs as if fully set forth below.

162. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for

Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PII/PHI; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

163. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

164. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

165. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII/PHI.

166. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

167. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII/PHI;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: May 29, 2024

Respectfully submitted,

By: /s/ Raina C. Borrelli

STRAUSS BORRELLI PLLC

Samuel J. Strauss
Raina Borrelli
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiffs and Proposed Class